

10/541510

DOCKET NO.: 274880US2PCT

JC20 Rec'd PCT/PTO 08 JUL 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Gilles MERLE, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/FR03/50202

INTERNATIONAL FILING DATE: December 22, 2003

FOR: METHOD AND SYSTEM FOR SECURING SCRAMBLED DATA

REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION

Commissioner for Patents
Alexandria, Virginia 22313

Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY
France

APPLICATION NO
02 16650

DAY/MONTH/YEAR
24 December 2002

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/FR03/50202.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak
Attorney of Record
Registration No. 24,913
Surinder Sachar
Registration No. 34,423

Customer Number
22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 08/03)



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 1.6 APR 2004

COPIE OFFICIELLE

WIPO PCT

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 23 JAN. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

**PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)**

Martine PLANCHE

**INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE**

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

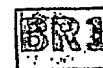
Code de la propriété intellectuelle - Livre VI



N° 11354*03

REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

DS 540 v 1 / 210502

REMANSE DES PIÈCES DATE 24 DEC 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0216650 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE 24 DEC. 2002 PAR L'INPI		<input checked="" type="checkbox"/> NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE BREVALEX 3, rue du Docteur Lancereaux 75008 PARIS	
Vos références pour ce dossier (facultatif) SP 22237 HM			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
<input checked="" type="checkbox"/> NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
ou demande de certificat d'utilité initiale		N° _____ Date _____	
Transformation d'une demande de brevet européen		<input type="checkbox"/> N° _____ Date _____	
Demande de brevet initiale			
TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCEDE ET SYSTEME DE SECURISATION DE DONNEES EMBROUILLEES			
DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		VIACCESS	
Prénoms			
Forme juridique		Société anonyme	
N° SIREN			
Code APE-NAF			
Domicile ou siège		Rue _____ Code postal et ville 92057 PARIS LA DEFENSE CEDEX Pays FRANCE française	
Nationalité			
N° de téléphone (facultatif)		N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page

**BREVET D'INVENTION
CERTIFICAT D'UTILITÉ**

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

REMISE DES PIÈCES OATE 24 DEC 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0216650 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	
6 MANDATAIRE (s'il y a lieu) Nom DU BOISBAUDRY Prénom Dominique Cabinet ou Société BREVALEX N° de pouvoir permanent et/ou de lien contractuel Adresse Rue 3, rue du Docteur Lancereaux Code postal et ville 75 008 PARIS Pays FRANCE N° de téléphone (facultatif) 01 53 83 94 00 N° de télécopie (facultatif) 01 45 63 83 33 Adresse électronique (facultatif) brevets.patents@brevaalex.com			
7 INVENTEUR (S) Les demandeurs et les inventeurs sont les mêmes personnes <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)		Les inventeurs sont nécessairement des personnes physiques	
8 RAPPORT DE RECHERCHE Établissement immédiat ou établissement différé <input checked="" type="checkbox"/> Établissement immédiat <input type="checkbox"/> Établissement différé Paiement échelonné de la redevance (en deux versements) <input type="checkbox"/> Oui <input type="checkbox"/> Non		Uniquement pour une demande de brevet (y compris division et transformation) Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt	
9 RÉDUCTION DU TAUX DES REDEVANCES <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence): AG		Uniquement pour les personnes physiques	
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS Le support électronique de données est joint <input type="checkbox"/> Oui <input type="checkbox"/> Non La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe <input type="checkbox"/> Oui <input type="checkbox"/> Non Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) D. DU BOISBAUDRY CPI 950304		VISA DE LA PRÉFECTURE OU DE L'INPI	

**PROCEDE ET SYSTEME DE SECURISATION DE DONNEES
EMBROUILLEES**

DOMAINE TECHNIQUE

L'invention se situe dans le domaine du
5 contrôle d'accès à des données embrouillées.

Elle concerne plus spécifiquement un procédé de
sécurisation de données embrouillées fournies à une
pluralité de terminaux munis chacun d'un processeur de
sécurité.

10 Les terminaux récepteurs sont des équipements
mobiles (ME) (pour Mobile Equipment en anglais) à usage
grand public tels que par exemple des téléphones
portables, des assistants numériques personnels appelés
PDA (pour Personal Digital Assistant en anglais) ou
15 encore des récepteurs audiovisuels ou des ordinateurs.

L'invention concerne également un système de
sécurisation de données et/ou services comportant une
plate-forme d'embrouillage et une plate-forme de
désembrouillage destinées à mettre en œuvre le procédé.

20 Les données à sécuriser sont des œuvres
littéraires ou artistiques protégées par un système
numérique de gestion de droits DRM (pour Digital Right
Management). Ces œuvres peuvent être soit mémorisées
sur un support tel que par exemple un CD ROM ou un DVD,
25 soit transmises ou téléchargées à partir d'un serveur
distant vers une pluralité de terminaux récepteurs
connectés à un réseau de transmission.

ETAT DE LA TECHNIQUE ANTERIEURE

30 Dans les systèmes de sécurisation de données de
l'art antérieur, le contenu à protéger (audio, vidéo,

texte...) est embrouillé chez l'opérateur et déchiffré lors de sa réception chez l'abonné par un algorithme de désembrouillage mémorisé dans le terminal récepteur.

Un inconvénient majeur de ces systèmes provient
5 du fait qu'à la réception, tout le contenu distribué est désembrouillé par un même module de désembrouillage. Aussi, en cas de piratage, la totalité de ce contenu devient accessible et peut alors être redistribué frauduleusement sur des réseaux illicites.

10 Une première solution connue pour pallier à ce problème consiste à confiner le module de désembrouillage dans un local à accès sécurisé. Cette solution n'est pas adaptée aux applications dans lesquelles les terminaux sont à usage grand public.

15 Une deuxième solution, basée sur le renforcement de la sécurité du récepteur lui-même, consiste à empêcher l'installation sur le terminal de tout logiciel suspect et d'autoriser l'installation uniquement de logiciels « certifiés », c'est-à-dire,
20 des logiciels pour lesquels une autorisation de téléchargement a été donnée.

Cette solution n'est pas non plus adaptée aux applications citées ci-dessus qui utilisent des récepteurs « ouverts » munis d'une interface d'entrée
25 sortie permettant de télécharger tout type de logiciels (ordinateurs, récepteurs audio et vidéo) par opposition aux terminaux « verrouillés » par fabrication, tels que les décodeurs par exemple, pour empêcher un abonné de télécharger frauduleusement des logiciels de
30 désembrouillage.

Le but de l'invention est de pallier les inconvénients de l'art antérieur cités ci-dessus.

EXPOSÉ DE L'INVENTION

5 L'invention préconise un procédé de sécurisation de données embrouillées fournies à une pluralité de terminaux récepteurs.

Ce procédé comporte :

- une première phase de chiffrement comprenant les
10 étapes suivantes :
 - . subdiviser lesdites données en un nombre entier de familles F_j ($j=1..M$) comportant chacune un nombre entier de blocs B_i ($i=1..N$),
 - . affecter à chaque famille F_j un paramètre
15 spécifique d'identification p_j ($j=1..M$) associé à au moins un module de désembrouillage M_j ayant une capacité de traitement et un niveau de sécurité spécifiques,
 - . embrouiller chaque bloc B_i d'une famille F_j de
20 type p_j par une clé K_j ($j=1..M$) en relation biunivoque avec le paramètre p_j ,
- et une deuxième phase de désembrouillage comportant les étapes suivantes :
 - . identifier la famille de chaque bloc B_i ,
 - 25 . désembrouiller chaque bloc B_i d'une famille de type p_j par le module M_j au moyen de la clé K_j .

Selon l'invention, les modules M_j ($j=1..M$) sont des éléments périphériques différents associés audit terminal récepteur.

Grâce à l'invention, une attaque sur l'un des modules M_j ($j=1..M$) permet de reconstruire un fichier qui n'est pas complet car il manque la partie traitée par les autres modules. Le fichier piraté sera
 5 fortement dégradé par rapport à l'original et donc inexploitable.

Dans un premier mode de réalisation, les modules de désembrouillage M_j ($j=1..M$) comportent des algorithmes A_j ($j=1..M$) différents.

10 Dans un deuxième mode de réalisation les modules de désembrouillage M_j ($j=1..M$) comportent des algorithmes A_j ($j=1..M$) identiques.

Dans les deux modes de réalisation, les données à distribuer se présentent sous forme d'un fichier
 15 préalablement mémorisé ou sous forme d'un flux diffusé en temps réel.

Dans une application particulière du procédé selon l'invention, le flux de données représente des programmes audio et/ou vidéo ou des dessins animés
 20 (animation multimédia), ou encore des images de synthèses protégées par un système DRM.

L'invention concerne également un système de sécurisation de données embrouillées comportant une plate-forme d'embrouillage et une plate-forme de
 25 désembrouillage.

La plate-forme d'embrouillage comporte:

- des moyens pour subdiviser ledit flux en m familles distinctes de N blocs B_i ($i=1..N$),
- des moyens pour affecter à chaque famille un
 30 paramètre spécifique d'identification p_j ($j=1..M$) associé à au moins un module de désembrouillage M_j

ayant une capacité de traitement et un niveau de sécurité spécifiques,

- des moyens pour embrouiller chaque bloc B_i par une clé K_j ($j=1..M$) en relation biunivoque avec le paramètre p_j .

Selon une caractéristique essentielle de l'invention, ladite plate-forme de désembrouillage comporte des moyens pour identifier la famille de chaque bloc B_i de manière à désembrouiller chaque bloc B_i d'une famille de type p_j par le module M_j correspondant audit paramètre p_j .

Selon un mode préféré de réalisation, la plate-forme de désembrouillage comporte une pluralité de modules de désembrouillage distincts M_j ($i=1..M$).

Dans une variante de réalisation de l'invention, les données à sécuriser sont des programmes audiovisuels diffusés à une pluralité d'abonnés munis de licence d'utilisation gérée par un système DRM.

L'équipement mobile peut être un PDA ou un téléphone mobile muni d'une carte à puce de type SIM (pour Subscriber Identity Module, en anglais).

Dans ce cas, les données sont réparties entre un premier module de désembrouillage M_1 intégré dans le PDA (respectivement dans le téléphone mobile) et un deuxième module de désembrouillage M_2 constitué par la carte à puce elle-même.

BRÈVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va

suivre, prise à titre d'exemple non limitatif en référence aux figures annexées dans lesquelles :

- la figure 1 illustre schématiquement une étape de typage de données à sécuriser par le procédé selon l'invention,
- la figure 2 illustre schématiquement une étape d'embrouillage d'une famille de données obtenue par l'étape précédente,
- la figure 3 illustre schématiquement un premier mode de réalisation de la première et de la deuxième étape du procédé selon l'invention,
- la figure 4 représente schématiquement la phase de désembrouillage des familles de données obtenues par les étapes précédentes,
- - la figure 5 représente un mode préféré de réalisation de l'étape illustrée par la figure 4,
- - la figure 6 représente schématiquement un terminal mettant en œuvre le procédé selon l'invention,
- la figure 7 représente un diagramme temporel illustrant schématiquement le traitement par le procédé selon l'invention d'un flux de données diffusées ou téléchargé en temps réel par le terminal,
- la figure 8 représente un diagramme temporel illustrant la gestion des clés d'embrouillage du flux de la figure 7.

EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

La description qui suit concerne une application de l'invention dans laquelle les données embrouillées représentent des programmes audio et/ou

vidéo diffusés ou téléchargés vers un PDA (pour
 Personal Digital Assistant) muni d'une carte à puce de
 type SIM. Le PDA comporte un premier module M1 de
 désembrouillage, un deuxième module de désembrouillage
 5 étant la carte SIM elle-même.

Les données à sécuriser peuvent être
 téléchargées à partir d'un support d'enregistrement
 (CD, DVD...) ou à partir d'un serveur spécialisé
 (Musique, vidéo, dessins animés, sonneries
 10 téléphoniques, livre électronique E-Book...).
 Elles peuvent également être diffusées dans un réseau.

Quels que soient l'application envisagée et le
 type de données, avant la distribution de ces données,
 le procédé comporte :

- 15 - une première phase de traitement comportant :
 - une étape de typage consistant à former m familles F_j ($j = 1..M$) de données comportant chacune un nombre n_j blocs de données B_i ($i = 1..N$), chaque famille étant identifiée par un paramètre p_j .
 - 20 • une étape d'embrouillage de chaque bloc B_i d'une famille F_j par une clé K_j ($j = 1..M$) en relation biunivoque avec le paramètre p_j .
- et à réception des données par un terminal, celles-ci subissent une deuxième phase de traitement
- 25 comportant :
 - une étape d'identification de la famille de chaque bloc B_i reçu,
 - une étape de désembrouillage de chaque bloc B_i au moyen de la clé K_j par un module M_j ($j = 1..M$)
 - 30 identifié par un paramètre p_j .

Selon une caractéristique essentielle de l'invention, les module M_j ($j=1...M$) qui permettent de désembrouiller les blocs B_i de deux familles distinctes sont différents.

5 Ceux-ci peuvent être soit des périphériques différents associés au terminal récepteur, ou des logiciels indépendants stockés dans la mémoire du terminal ou d'un périphérique.

10 Cas d'un fichier de données préalablement mémorisé.

Typage

La figure 1 représente un fichier 2 de données audio et/ou vidéo organisées en blocs appelés unités
15 d'accès AU (pour Access Unit) selon la norme MPEG 4 (pour Motion Picture Expert Group).

Une première étape 4 du procédé consiste à découper le fichier 2 en m familles F_j ($j=1...m$) comportant chacune un nombre entier n_j de blocs B_i
20 ($i=1...N$); Chaque famille F_j est identifiée par paramètre p_j ($j=1...m$).

Le paramètre p_j identifie également le module M_j qui sera chargé de désembrouiller les blocs B_i de la famille F_j .

25 Dans l'application décrite, le fichier est découpé en deux familles F_1 et F_2 dont les blocs respectifs seront désembrouillés respectivement par un module M_1 intégré au PDA et par la carte SIM constituant le module M_2 .

30 Lors du typage, un paramètre p_1 est associé à la famille F_1 de blocs B_i qui seront désembrouillés par

le module M_1 et un paramètre p_2 est associé à la famille F_2 de blocs B_i qui seront désembrouillés par la carte SIM.

5 Embrouillage

La figure 2 illustre une deuxième étape 6 au cours de laquelle les blocs B_i d'une famille F_j sont embrouillés par une clé K_j ($j=1,2$) définie en fonction de la capacité de traitement et du degré de sécurité respectifs du module M_1 intégré au PDA et de la carte SIM. Les blocs embrouillés B'_i sont stockés dans un fichier 8.

Dans une variante de réalisation du procédé illustrée schématiquement par la figure 3, le typage 4 et l'embrouillage 6 d'un bloc B_i sont réalisés successivement.

Dans une autre variante de réalisation non représentée, l'embrouillage est réalisé famille par famille.

Le fichier 10 contenant les blocs B'_i embrouillés est ensuite transmis au PDA.

Désembrouillage

La figure 4 illustre la phase de désembrouillage d'un fichier 10 comportant des familles F_j distinctes de blocs MPEG préalablement embrouillés.

A l'étape 12, les blocs B'_i sont identifiés par leur paramètre respectif p_j puis aiguillés sur les modules de désembrouillage correspondant M_j .

Les blocs déchiffrés sont ensuite réarrangés pour former le fichier d'origine 2 qui sera fourni à l'utilisateur.

La figure 5 illustre schématiquement un mode préféré de réalisation du désembrouillage dans lequel les blocs Bi contenus dans le fichier 10 sont traités à la volée bloc par bloc.

Traitement temporel d'un flux de données

10

La figure 6 représente schématiquement les modules internes d'un PDA permettant de réaliser le désembrouillage.

Le PDA illustré comporte un étage d'entrée 20 chargé d'identifier les blocs B'i dans un flux, un étage 22 de démultiplexage, un premier module de désembrouillage 24, une carte à puce constituant un deuxième module de désembrouillage 26, un étage de multiplexage 28 et un étage de sortie 30.

20 La figure 7a illustre schématiquement un flux de données diffusé ou téléchargé comportant des blocs Bi au format MPEG 4.

Un premier traitement de ce flux, réalisé au niveau de l'émetteur, consiste à réorganiser les blocs MPEG en fonction des capacités et des vitesses respectives de traitement du module M1 et de la carte SIM.

La figure 7b représente le flux de la figure 7a dans laquelle ont été créées une famille formée par des blocs de type A et une famille formée par des blocs de type B.

Dans cet exemple, les blocs de type A seront désembrouillés par le module M1 et les blocs de type B par la carte SIM.

5 Du fait que la capacité et la vitesse de traitement de la carte SIM sont inférieures à celles du décodeur, à l'émission, les blocs de type B sont décalés de trois blocs en amont de manière à compenser la différence de vitesse de traitement entre le décodeur et la carte SIM.

10 La figure 7c représente la répartition temporelle des blocs du flux diffusé après embrouillage et réorganisation.

La figure 7d représente la répartition temporelle des blocs du flux reçus par le PDA avant désembrouillage, et la figure 7e représente la répartition temporelle des blocs du flux désembrouillé.

La figure 8 illustre schématiquement le mécanisme de changement de clés pour désembrouiller les blocs du flux traité.

20 On désigne par crypto-période la durée de validité d'une clé de désembrouillage. Avant chaque début de crypto-période un message est inséré dans le flux afin de prévenir le module de désembrouillage du changement de crypto-période. Ce message contient
25 l'ensemble des informations nécessaires pour désembrouiller le flux pendant la crypto-période suivante (par exemple la référence de la clé de désembrouillage à utiliser). Ce message est inséré dans le flux avant le début de la crypto-période (delay
30 start) afin de permettre au module de désembrouillage de traiter les informations du message et d'être prêt à

désembrouiller en temps réel les données de la crypto-période à venir.

Les Applications

5 Cette invention s'applique à des contenus où la perte d'une partie de l'information rend le contenu inexploitable. Cela s'applique à l'ensemble des contenus audio et vidéo numériques compressés où la perte d'information se traduit par une dégradation
10 rapide de la qualité (audio, vidéo, Ebook, sonneries de téléphones portable, image..).

Les modules de déchiffrement visés sont :

- des supports amovibles type carte à puce, carte à puce sans contact, module détachable (PCMCIA, série,
15 USB, Ethernet).
- des terminaux type PC, serveur, décodeur numérique, récepteur mobile (Téléphone Mobile, PDA).

Les services :

- 20 - VOD (Video On Demand) en diffusion ou en téléchargement,
- MOD (Music On Demand) en diffusion ou en téléchargement,
- Diffusion de livre électronique en ligne,
- 25 - Diffusion de sonnerie pour téléphone mobile,
- Diffusion de photo/image,
- Diffusion de texte, document multimédia.

REVENDICATIONS

1. Procédé de sécurisation de données embrouillées fournies à au moins un terminal récepteur, caractérisé en ce qu'il comporte :

- 5 - une première phase de chiffrement comprenant les étapes suivantes :
- subdiviser lesdites données en un nombre entier de familles F_j ($j=1..M$) comportant chacune un nombre entier de blocs B_i ($i=1..N$),
 - 10 • affecter à chaque famille F_j un paramètre spécifique d'identification p_j ($j=1..M$) associé à au moins un module de désembrouillage M_j ayant une capacité de traitement et un niveau de sécurité spécifiques,
 - 15 • embrouiller chaque bloc B_i d'une famille F_j de type p_j par une clé K_j ($j=1..M$) en relation biunivoque avec le paramètre p_j ,
- et une deuxième phase de désembrouillage comportant les étapes suivantes :
- 20 • identifier la famille de chaque bloc B_i ,
 - désembrouiller chaque bloc B_i d'une famille de type p_j par le module M_j au moyen de la clé K_j .

2. Procédé selon la revendication 1, caractérisé en ce que les modules M_j ($j=1..M$) sont des éléments périphériques différents associés audit terminal récepteur.

3. Procédé selon la revendication 2, caractérisé en ce que les modules de désembrouillage M_j

(j=1...M) comportent des algorithmes A_j (j=1...M) différents.

4. Procédé selon la revendication 2, caractérisé en ce que les module de désembrouillage M_j (j=1...M) comportent des algorithmes A_j (j=1...M) identiques.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à distribuer se présentent sous forme d'un fichier préalablement mémorisé.

6. Procédé selon l'une des revendications 1 à 4, caractérisé en ce que les données à sécuriser se présentent sous forme d'un flux diffusé ou téléchargé et traité en temps réel par le terminal.

7. Procédé selon les revendications 5 ou 6, caractérisé en ce que la durée d'utilisation du flux est divisée en crypto-périodes correspondant chacune à une clé de désembrouillage, et en ce qu'avant chaque début de crypto-période un message est inséré dans le flux afin de prévenir le module de désembrouillage M_j du changement de crypto-période.

8. Procédé selon la revendication 7, caractérisé en ce que ledit message comporte l'ensemble des informations nécessaires pour désembrouiller le flux utilisé pendant la crypto-période suivante.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent des programmes audio et/ou vidéo protégés par un système DRM.

5

10. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que lesdites données représentent des images de synthèse ou des dessins animés.

10 11. Système de sécurisation de données embrouillées fournies à au moins un terminal récepteur, caractérisé en ce qu'il comporte :

- une plate-forme d'embrouillage comprenant :

- 15 . des moyens pour subdiviser lesdites données en m familles distinctes de N blocs B_i ($i=1..N$),
- 15 . des moyens pour affecter à chaque famille F_j un paramètre spécifique d'identification p_j ($j=1..M$) associé à au moins un module de désembrouillage M_j ayant une capacité de traitement et un niveau de
- 20 sécurité spécifiques,
- 20 . des moyens pour embrouiller chaque bloc B_i par une clé K_j ($j=1..M$) en relation biunivoque avec le paramètre p_j ,

- et une plate-forme de désembrouillage comportant des

25 moyens pour identifier la famille de chaque bloc B_i de manière à désembrouiller chaque bloc B_i d'une famille de type p_j par le module M_j correspondant audit paramètre p_j .

30 12. Système selon la revendication 11, caractérisé en ce que les modules de désembrouillages

distincts M_j ($j=1..M$) sont des périphériques distincts associés au terminal récepteur.

13. Plate-forme d'embrouillage d'un flux de données, caractérisée en ce qu'elle comporte :
- des moyens pour subdiviser ledit flux en m familles distinctes de N blocs B_i ($i=1..N$),
 - des moyens pour affecter à chaque famille un paramètre spécifique d'identification p_j ($j=1..M$) associé à au moins un module de désembrouillage M_j ayant une capacité de traitement et un niveau de sécurité spécifiques,
 - des moyens pour embrouiller chaque bloc B_i par une clé K_j ($j=1..M$) en relation biunivoque avec le paramètre p_j .

14. Plate-forme de désembrouillage d'un flux de données embrouillé par la plate-forme de la revendication 13, caractérisée en ce qu'elle comporte des moyens pour identifier la famille de chaque bloc B_i de manière à désembrouiller chaque bloc B_i d'une famille de type p_j par le module M_j correspondant audit paramètre p_j .

15. Plate-forme de désembrouillage selon la revendication 14, caractérisée en ce qu'elle comporte une pluralité de modules de désembrouillage distincts M_j ($i=1..M$) identifiés chacun par le paramètre spécifique d'identification p_j .

16. Plate-forme de désembrouillage selon la revendication 15, caractérisée en ce que le terminal récepteur est un PDA et en ce que l'un desdits modules de désembrouillage M_j ($i=1..M$) est intégré au PDA et au moins deuxième module est une carte à puce de type SIM connectée audit PDA.

17. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de vidéo à la demande (VOD).

18. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser un service de Musique à la demande (MOD).

15

19. Utilisation du procédé selon l'une des revendications 1 à 8 pour sécuriser l'accès à un service diffusion de livre électronique en ligne ou téléchargé à partir d'un support amovible.

20

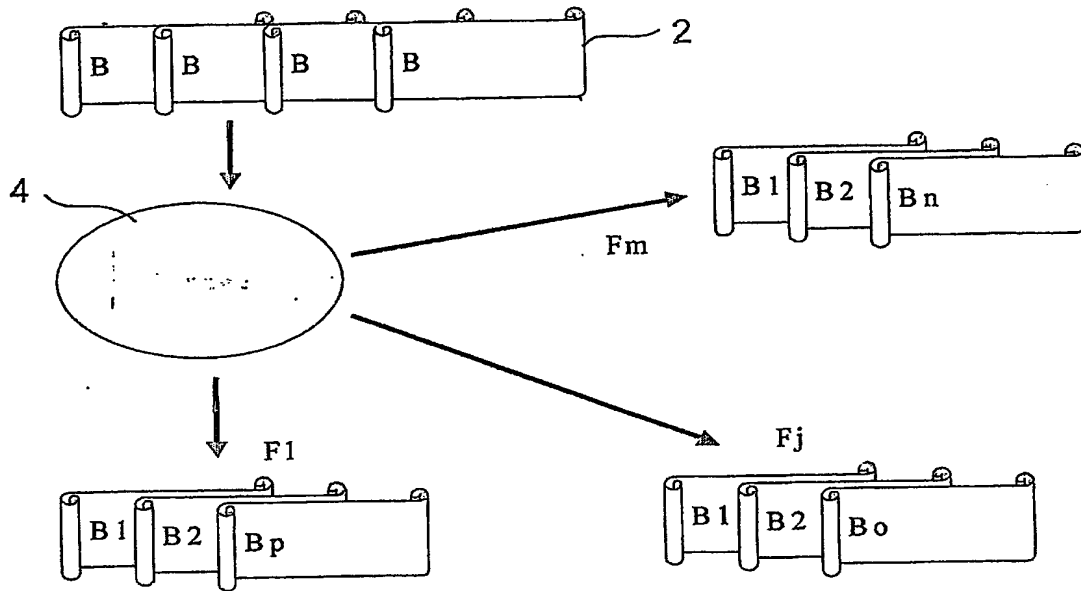


FIG. 1

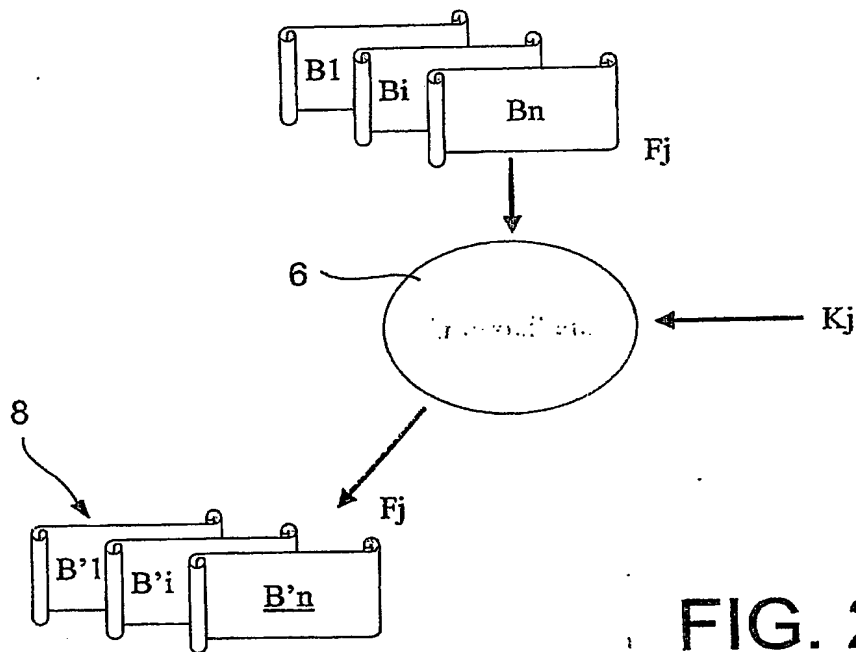


FIG. 2

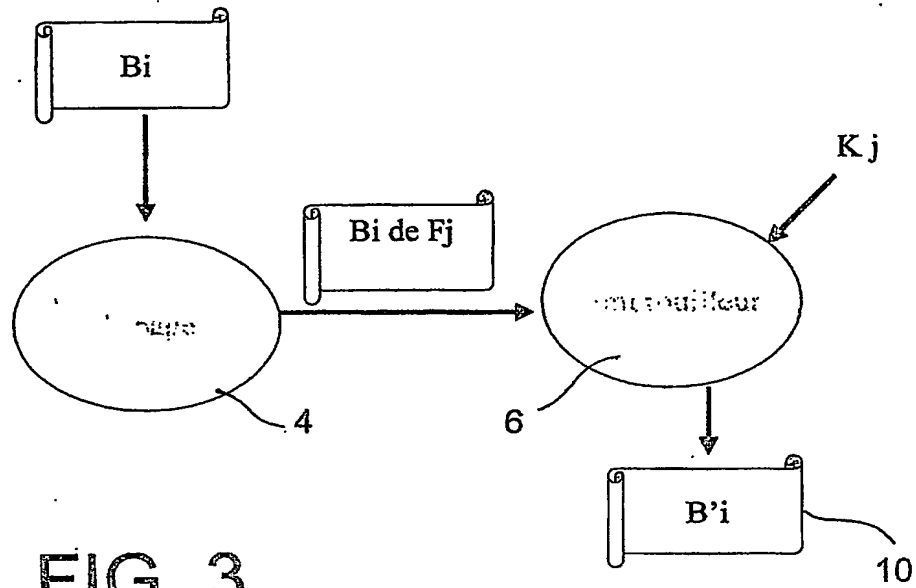


FIG. 3

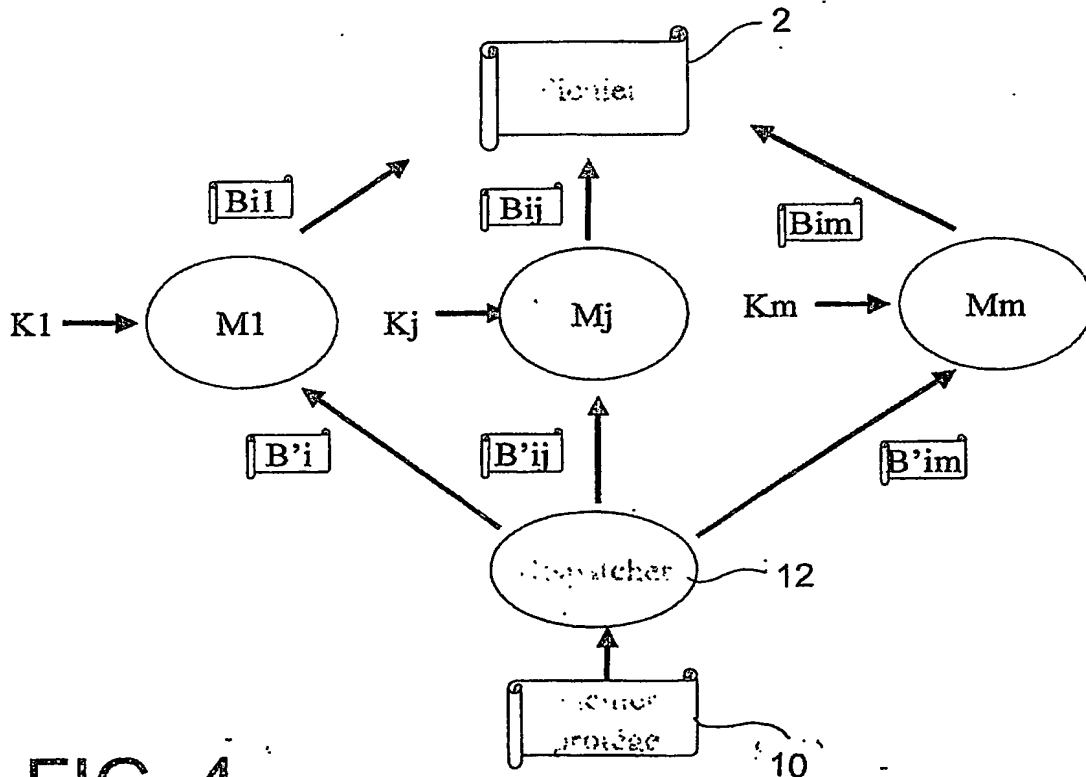


FIG. 4

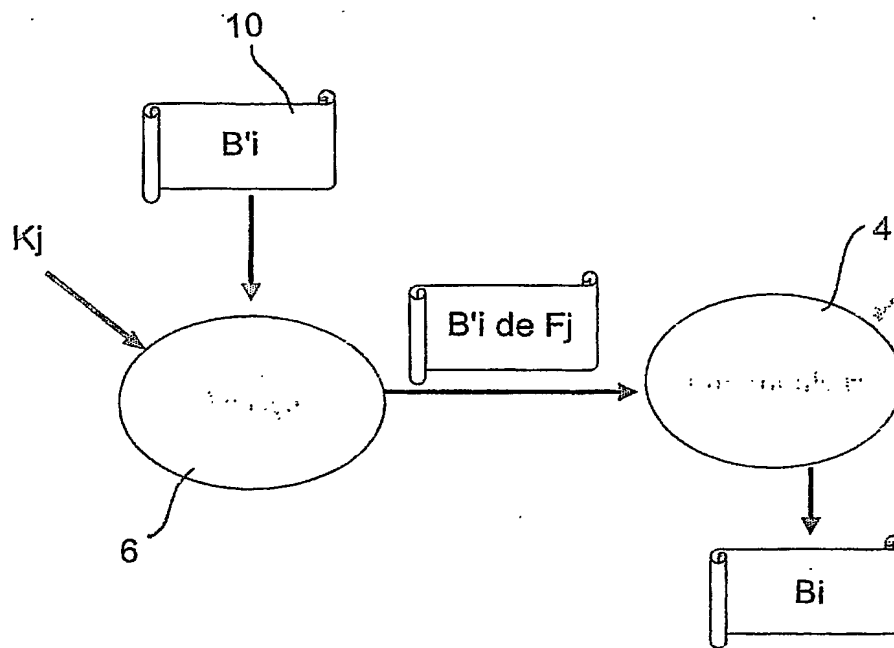


FIG. 5

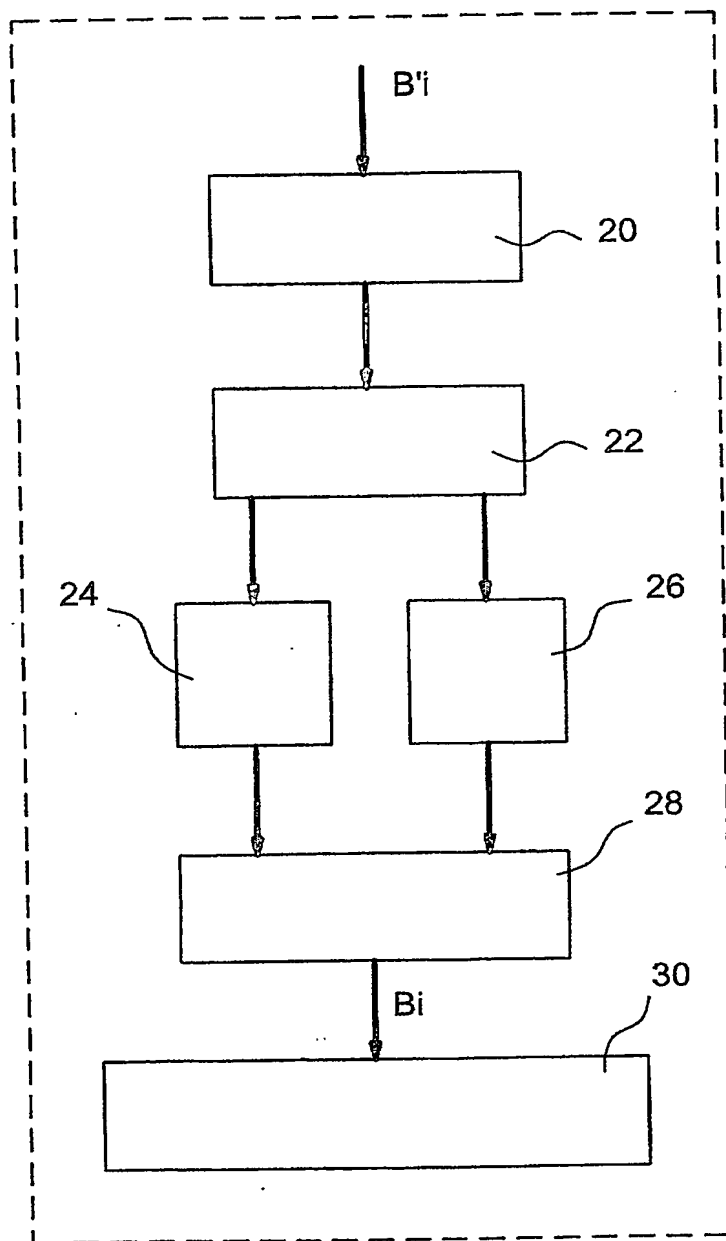
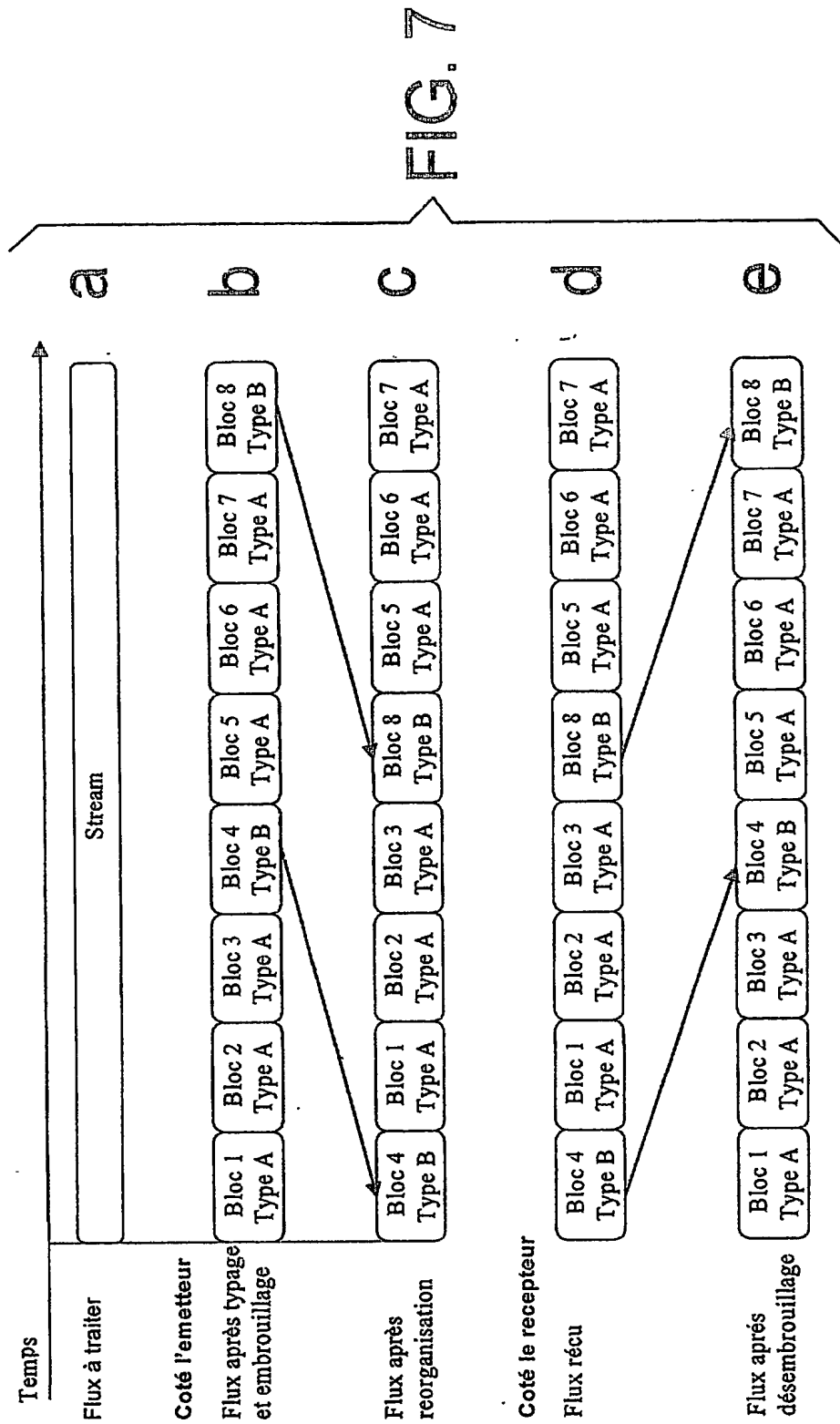


FIG. 6



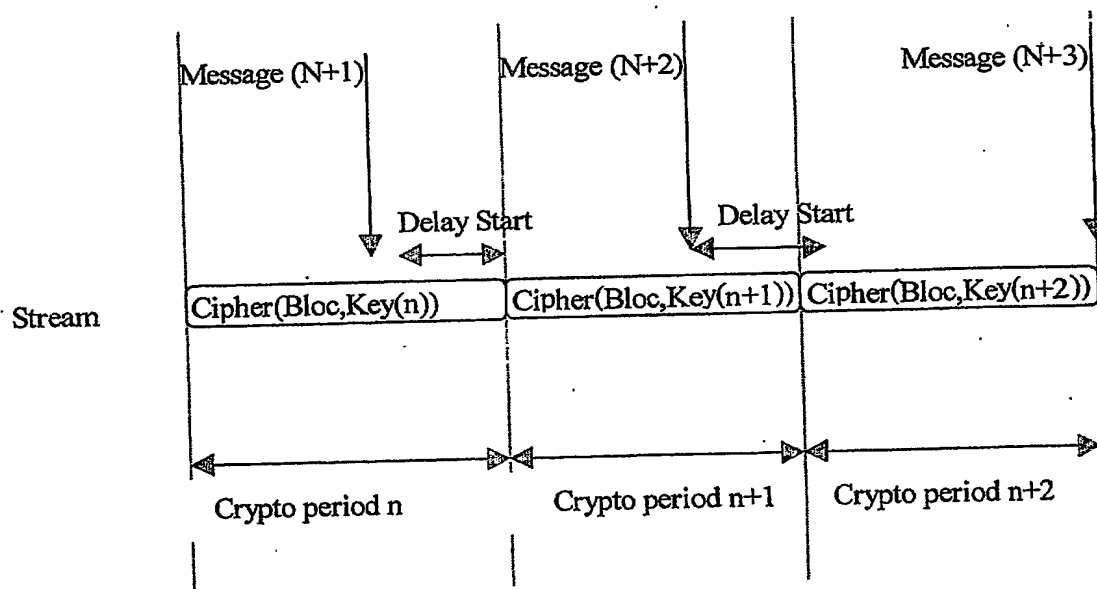


FIG. 8

**BREVET D'INVENTION****CERTIFICAT D'UTILITÉ**

Code de la propriété intellectuelle - Livre VI

**DÉPARTEMENT DES BREVETS**

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

(À fournir dans le cas où les demandeurs et
les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 6 W / 270601

Vos références pour ce dossier (facultatif)		SP 22237/HM
N° D'ENREGISTREMENT NATIONAL		02.16650 DU 24.12.2002
TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCEDE ET SYSTEME DE SECURISATION DE DONNEES EMBROUILLEES.		
LE(S) DEMANDEUR(S) : VIACCESS Les collines de l'Arche - Tour Opéra C 92057 PARIS LA DEFENSE CEDEX		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :		
<input checked="" type="checkbox"/> 1	Nom	MERLE
	Prénoms	Gilles
Adresse	Rue	41 rue du Hameau
	Code postal et ville	718141810 VERNEUIL SUR SEINE
Société d'appartenance (facultatif)		
<input checked="" type="checkbox"/> 2	Nom	BANGUI
	Prénoms	François
Adresse	Rue	69 rue Dunois
	Code postal et ville	715161416 PARIS 13ème
Société d'appartenance (facultatif)		
<input checked="" type="checkbox"/> 3	Nom	
	Prénoms	
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire) PARIS LE 4 MARS 2003 J.C. ILGART		

PCY/FR003/050202

